Army Systems Realignment and Categorization (SRAC) Guide

July 2004

MESSAGE

16 July 2004

Dear Reader,

Our purpose in publishing this Systems Realignment and Categorization (SRAC) Guide is to assist you with conducting a 100 percent IT systems inventory and categorization of your systems so you can identify the "as-is" portfolio for your business domain. This guide walks you through the steps of the SRAC process using a proven methodology that allows you to identify what systems perform which functions in the current environment.

Once your "as-is" portfolio is identified, each domain will be able to move on to the next step in portfolio management (PfM)—consolidation of system requirements—where the domains will evaluate their legacy systems and prioritize them according to the benefit they bring to the Army. The domains will also review recommendations for new systems during this phase. New systems must support or modernize a strategic or operational requirement or capability that is not currently being supported, and they must align with the Army and the Domain's Strategic Plan.

By completing a full inventory of your business IT systems, you will have accomplished a key milestone that supports the DoD guidance on IT portfolio management. In turn, your efforts will support the Army's alignment to the Business Enterprise Architecture (BEA) and the Secretary of Defense's Business Management Modernization Program (BMMP).

I am confident this SRAC guide will be a valuable resource in your efforts to develop your "as-is" IT portfolio and operational architecture. I encourage you to use this guide to complete this extremely important task.

Carla A. von Bernewitz
Director, Army Enterprise Integration Oversight Office

FOREWORD

ARMY SYSTEMS REALIGNMENT AND CATEGORIZATION PROCEDURES

DoD recently published a new directive[1] on Information Technology Portfolio Management. This directive assigns responsibilities for managing information technology (IT) investments and states that IT investments shall be managed as portfolios. "Decisions on what IT investments to make, modify, or terminate shall be based on the Global Information Grid (GIG) Integrated Architectures, mission area goals, architectures, risk tolerance levels, potential returns, outcome goals and performance." The policy mandates that a portfolio management process will be established and will be comprised of four core activities: analysis, selection, control, and evaluation *(See Figure 1 pg. iv)*.

The Army Enterprise Integration Oversight Office (AEIOO) has the responsibility of enterprise integration oversight, which includes portfolio management oversight. AEIOO's organization aligns with the DoD business domains to facilitate oversight of the Army's Information Technology Portfolio of Investments. AEIOO ensures the Army business domains comply with both Army and DoD portfolio management requirements and align with public law and DoD and Army regulations.

The Army portfolio management process is a six-step process that mirrors DoD's four core PfM activities *(See Figure 1 pg. iv):*

- Review and develop the domain strategic plan, which is based on the Army Strategic Planning Guidance and the Army Campaign Plan.
- Inventory and categorize systems and update the Army Information Technology Registry (AITR).
- Consolidate system requirements and update the AITR.
- Develop enterprise architecture (EA) and planning and budgeting exhibits.
- Obtain Army approval—domain owner, CIO/G6, G8, and ASA(FM&C).

[1] Office of the Secretary of Defense, *Information Technology Portfolio Management,* 22 March 2004 (Enclosed).

SIX STEPS TO THE ARMY PfM PROCESS:

1. **Develop/Review Strategic Plan**
2. **Inventory Systems**
3. **Consolidate System Requirements**
4. **Develop EA, Planning, and Budget Documents**
5. **Obtain Army Approval**
6. **Obtain DoD Approval**

(See Figure 1 pg. iv)

- Obtain DoD approval—domain owner, Business Enterprise Architecture (BEA) Compliance Assessment, Business Modernization Systems Integration (BMSI), DoD CIO, and DoD Comptroller.

This document is concerned primarily with the second step in the IT portfolio management process: Inventory systems. The Systems Realignment and Categorization (SRAC) Guide was developed to help inventory and categorize domain systems. The unique methods of this web-based tool follow the first step in the portfolio management process: Development or review of the strategic plan.

Before domain owners can inventory their systems, they must develop a work breakdown structure (WBS), which will help them understand the functions and tasks supported by their systems.

SRAC provides a standard methodology for the collection and categorization of IT requirements for each domain's portfolio of systems—an important part of building and managing the portfolio. The SRAC procedure is tailored by each business domain to meet its specific domain requirements, with the end state a categorized list of IT assets. This information helps to document the system functionality, which provides the data required for the next step in the portfolio management process: Consolidate system requirements. In this next step, the SRAC results can be used when making key decisions about which systems will remain in the domain's portfolio.

Data collected during the SRAC process can be used as a starting point to develop the operational views (OV), system views (SV), and technical views (TV) using the Department of Defense Architecture Framework (DODAF) or other architecture tool that will represent the future Army Enterprise Architecture.

The information collected during the SRAC process can also be used to update the AITR and the initial operational view activity model (OV-5) under the DoD Business Management Modernization Program (BMMP) Transition Plan. Subsequent updates can employ the AITR update procedures or the domain's electronic tool.

This SRAC guide describes how to inventory and categorize the IT systems within a domain in order to make decisions about which systems should be retained, upgraded, or retired within the portfolio of systems. This guide—like the SRAC process—is divided into five phases that ensure the Army's universe of systems is carefully inventoried and analyzed *(See Figure 1 pg. iv):*

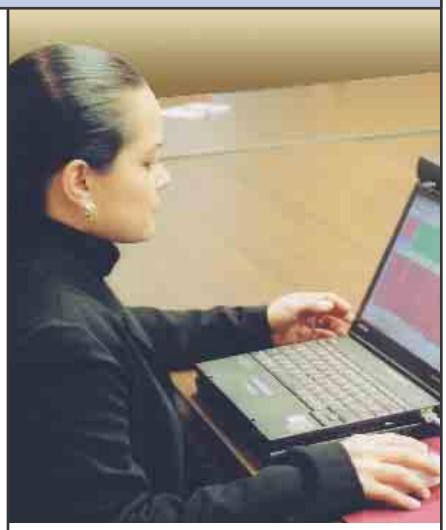
I. Conduct research and initial preparation

II. Develop the datacall

III. Conduct the datacall

IV. Categorize and analyze datacall results

V. Consolidate results and prepare final report

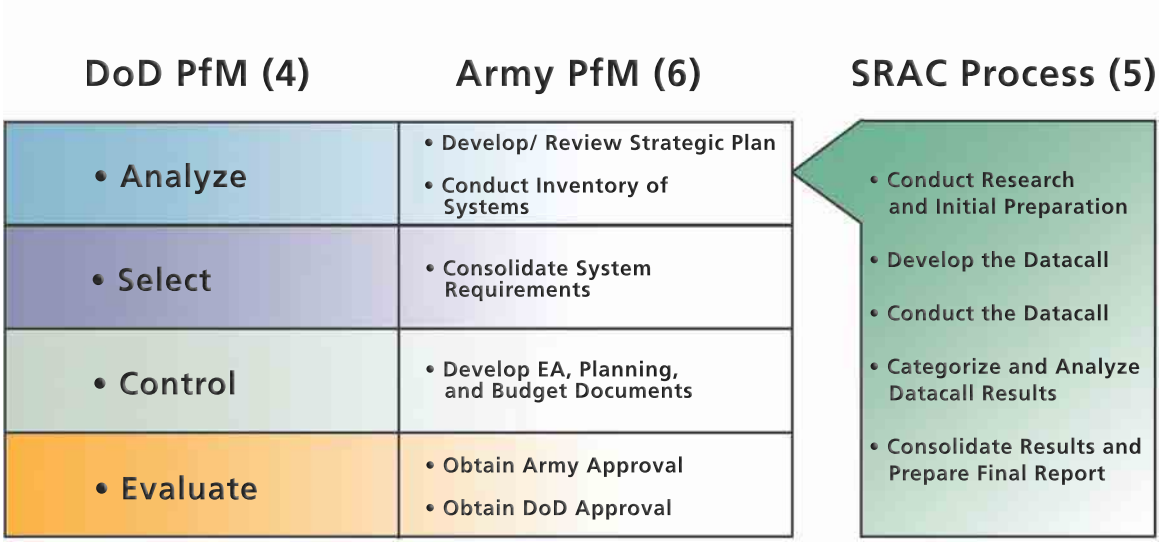


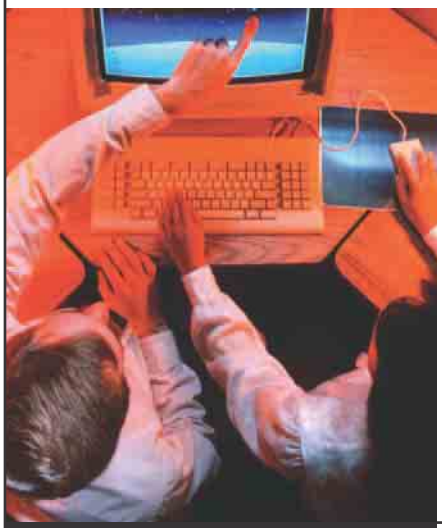
FIVE PHASES OF THE SRAC PROCESS:

1. **Conduct Research and Initial Preparation**
2. **Develop the Datacall**
3. **Conduct the Datacall**
4. **Categorize and Analyze Datacall Results**
5. **Consolidate Results and Prepare Final Report**

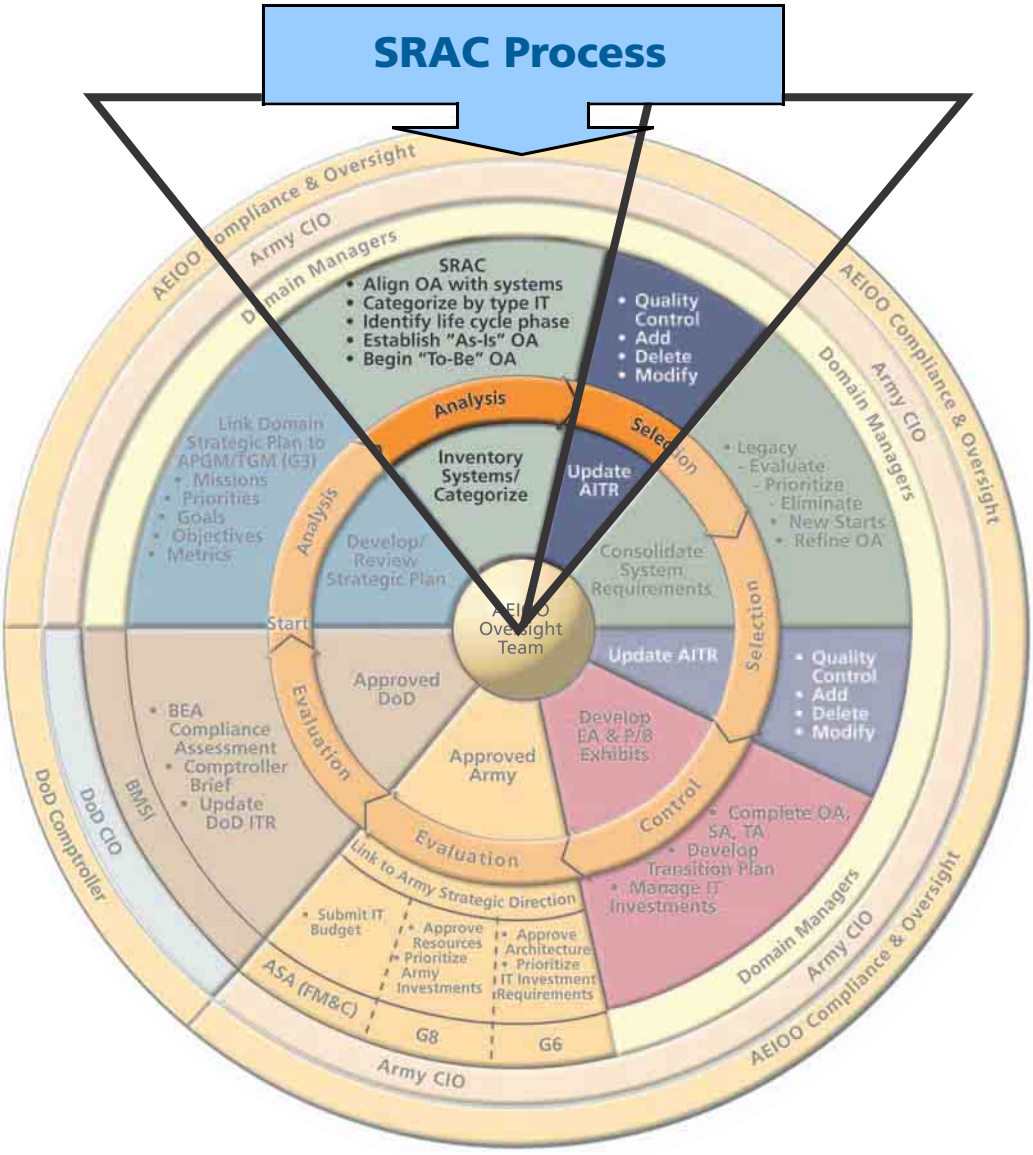
(See Figure 1 pg. iv)

FIGURE 1. CROSSWALK OF DoD CORE ACTIVITIES TO ARMY PORTFOLIO MANAGEMENT PROCESS AND SRAC PHASES





PORTFOLIO MANAGEMENT PROCESS



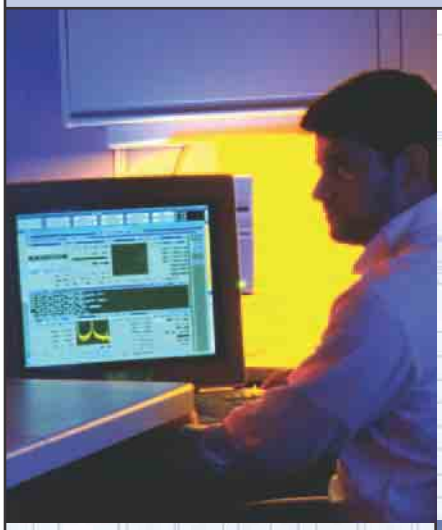
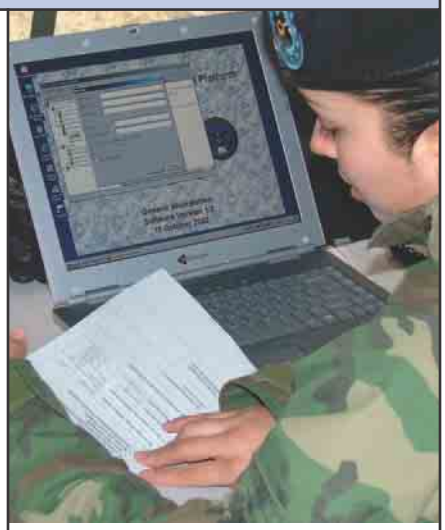
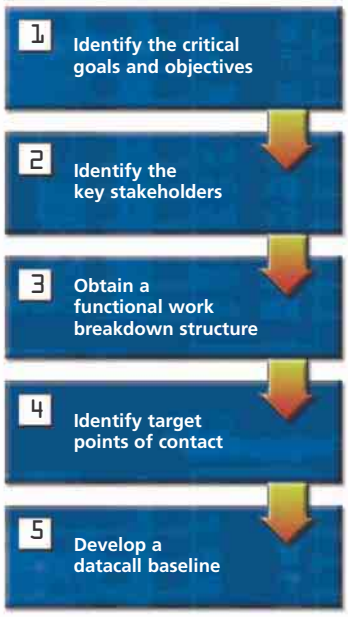


TABLE OF CONTENTS



PHASE I

CONDUCT RESEARCH AND INITIAL PREPARATION



This phase will give you the tools you need to successfully categorize the systems within your domain. It is the most critical phase of the SRAC. Regular communication between the Army's representative and the units or organizations that will answer the electronic datacall is imperative. Although the steps in this phase are often very time consuming, all of the requirements are necessary to successfully complete the datacall and the SRAC process.

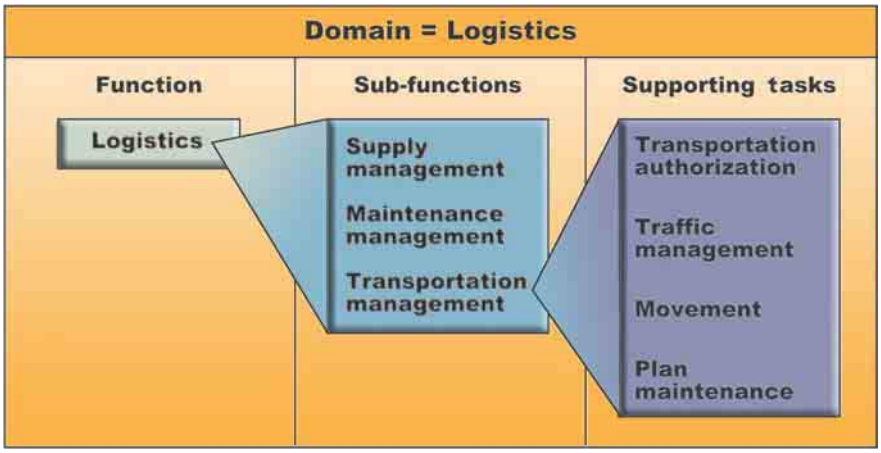
At the onset, **identify the critical goals and objectives** for the electronic datacall based on the needs of the domain and the Army. The SRAC team, those who administer the SRAC process, should have a clear understanding of the data that needs to be collected to support the goals and objectives. By staying focused on these requirements, the questions asked during the electronic datacall can be limited to only those that are necessary. This is important for maximizing the datacall participation and minimizing the time it takes to complete the datacall.

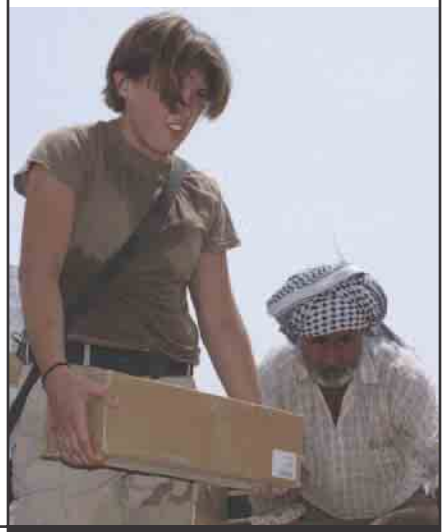
Based on the goals and objectives, the domain should use standard DoD or Army definitions for the IT information collected. These standard definitions should be annotated in the datacall.

Identify the key stakeholders for the SRAC project. This team must be capable of managing the project, tracking the timeline, developing the datacall questions, and analyzing and reporting the results. The team will also need a qualified software analyst capable of developing or selecting a web-based datacall.

Once the goals and objectives have been defined, the team should **obtain a functional work breakdown structure (WBS)**. The functional WBS is the high-level description of the functional requirements that the domain systems support. Many domains may be in the process of reengineering their business processes and developing functional WBS's; nonetheless, it is important to map legacy systems to a functional WBS that matches the functions of the legacy systems. If a functional WBS for your domain is not available, one must be built. The naming conventions for the first three functional levels should be functions, sub-functions, and supporting tasks. The function is the high-level task or domain (e.g., Logistics). The sub-functions equate to the missions that support the major function (e.g., supply management, maintenance management), and the supporting tasks are more specific tasks that support the sub-functions (transportation authorization, traffic management, etc.) *(See Figure 2)*.

FIGURE 2. NAMING CONVENTIONS



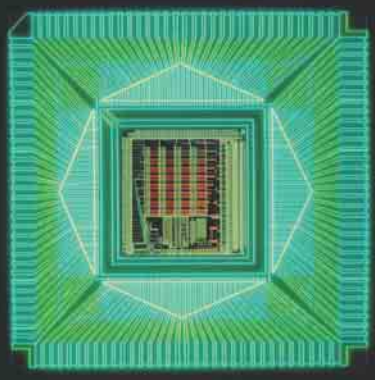


The domains should move toward a standard reference model to document the WBS. DoD has recently released a draft set of enterprise architecture reference models (including a Business Reference Model (BRM)) that are specific to DoD functions. The naming conventions of these reference models should be used. For more information, please visit the DoD Reference Model at *https://ca.dtic.mil/nii/ea/DoD/EA_Executive_Summary.htm.*

Identify target points of contact, those who will answer the datacall. First, it is important to know which organization you will target to answer the datacall. Second, identify who within these organizations should answer the datacall. Third, gather point of contact (POC) information on these organizations and people so you can communicate with these contacts in the future. Examples of organizations to target might include major commands (MACOMs), field operating agencies (FOAs), program executive offices (PEOs), and Headquarters Department of the Army (HQDA) staff. Who within the organization should answer the datacall depends upon what kind of information you are gathering. For example, if you are from the Accounting and Finance Domain, you should target the resource managers; if you are from the Logistics Domain, you should target the logistics managers *(See Figure 3).*

FIGURE 3. IDENTIFYING WHO SHOULD ANSWER THE DATACALL

Domain	Sample Organization	Directorate	Division
Finance and Accounting Logistics	TRADOC FORSCOM	G8 G4	Finance and Accounting Logistics

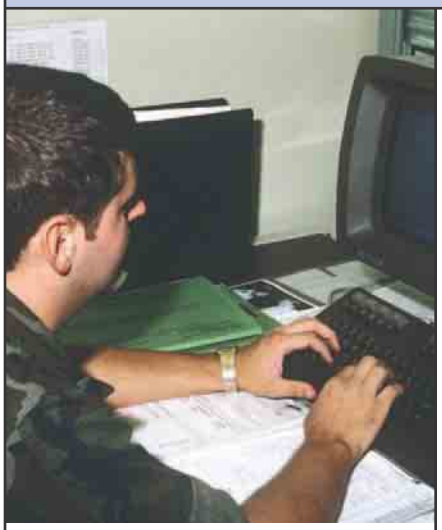


Develop the datacall baseline. To do so will require the collection of databases from a variety of authoritative sources (i.e., AITR, DoD Information Technology Registry (DoD ITR), and Information Technology Management Application (ITMA)). The domain subject matter experts (SMEs) should review the baseline for redundancy and accuracy. The baseline must contain an organization responsible for each system for validation. Once refined, the baseline will be used to populate the datacall with known systems.

After all of these steps are complete, you are ready to begin Phase II and develop the datacall.

PHASE II

DEVELOP THE DATACALL



1. Collect point of contact information
2. Determine how you will monitor your progress
3. Develop reminder letters
4. Determine how long to keep the datacall open

(continued on p. 7)

In this phase we complete a series of administrative tasks, develop a series of appropriate datacall questions, outline the datacall requirements, and program and test the datacall. At the close of Phase II you will be ready to implement a web-based datacall.

There are several administrative tasks that must be completed. Immediately following Phase I, **collect point of contact information** from targeted organizations. Prepare a letter announcing the datacall and asking for appropriate POCs. This letter should be signed by the domain owner to provide high-level emphasis. This is a time-consuming action as the letter takes time to staff, distribute, and receive responses. This process can take as little as 35 days, but may take much longer unless it is managed carefully. The letter need not be specific; leave the details of the datacall for the instruction letter that is transmitted with the initiation of the datacall in Phase III.

While you wait for points of contact, **determine how you will monitor the progress of the datacall.** It is important to identify who has completed the datacall, who has partially completed the datacall, and who has not started the datacall.

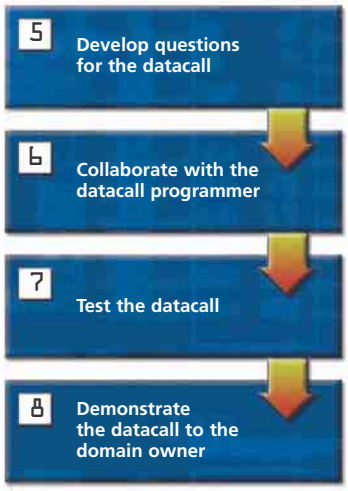
Develop reminder letters to send to participants who have not completed the datacall by set dates. Reminder form letters or e-mails should be sent at regular, programmed intervals throughout the datacall (e.g., halfway and three quarters of the way through) and should relay the number of working days remaining to meet the suspense date. Send out final notifications no later than 48 hours before the suspense date, remembering POC's are working in different times zones around the world.

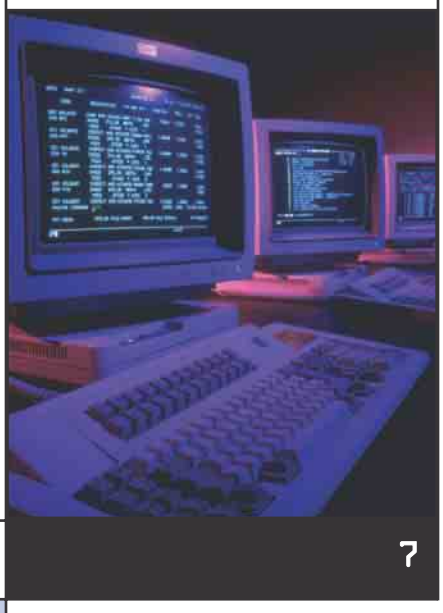
Identify how long you will keep the datacall open (30 calendar days is recommended). Interaction with participants is essential to the success of the datacall and will preclude the need for an extension. In fact, failure to communicate with the non-responsive organizations will jeopardize the quality of the data received for final SRAC analysis.

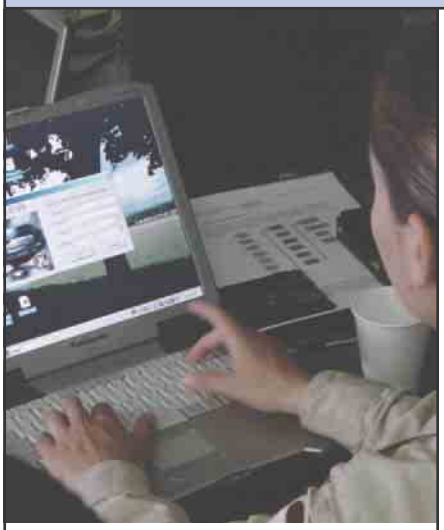
Once the administrative tasks are complete, **develop the questions for the datacall.** Questions should be based on the key goals and objectives identified in Phase I, and if these questions are in the AITR/DoD ITR, the answers on the datacall should map appropriately to these sources.

How you organize and phrase questions is as important as the questions you ask. Their order and phrasing should be logical and easy to follow. There should be four key sections in the datacall: POC information, update/edit systems on the baseline, add systems to the baseline, and comments. Additional sections can be added based on the domain's requirements.

There is flexibility in how the datacall is set up, so **collaboration with the datacall programmer or program analyst** is helpful when making development decisions. For example, who will answer the datacall, and how many levels will be built? The programmer can assign each MACOM a primary account to answer initial parts, and then set up analyst accounts so subordinate units can respond to latter parts. Another decision involves the authorization process. If a subordinate unit is answering the datacall, does the MACOM representative need to validate the entries?







After the domain conducts a full inventory of their systems and has good working knowledge of the systems in their portfolio, a government or commercial off-the-shelf tool can be used to manage and routinely update the domain portfolio.

Should the MACOM have oversight of the data or the completion requirements? These are just a few of the many questions that need to be asked, with answers provided to the programmer/program analyst in order to place the appropriate controls on the datacall.

Security requirements are another important consideration. Determine how screen names and passwords will be assigned and distributed, and what levels of control are necessary. Participants often forget passwords. The programmer can develop a help utility to assist in resetting these passwords.

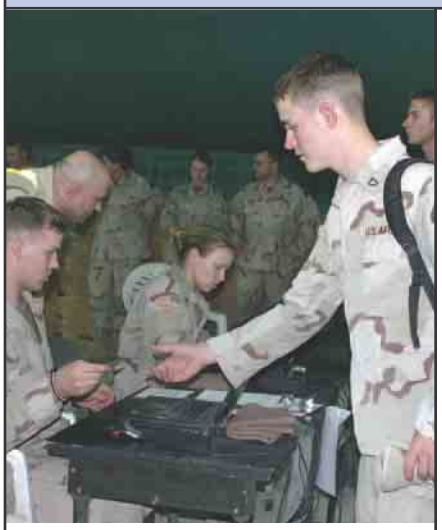
The programmer can assist in setting up a help desk to facilitate communication between participants and the SRAC help desk team. There are a number of ways to facilitate help during the datacall. The easiest is to provide the names, phone numbers, and e-mail addresses of the SRAC help desk team under a help desk button on the datacall. Another method is to have the programmer develop a utility that sends an e-mail directly the help desk. The help desk should be able to answer both functional and technical questions.

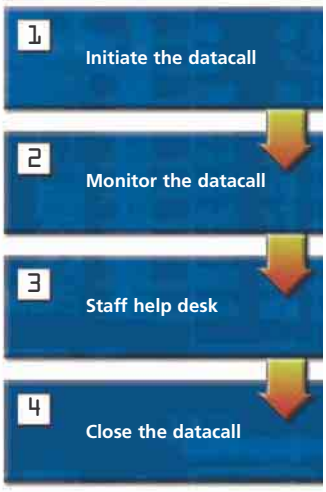
Remember to **test the datacall**—and all supporting technology—to ensure it works. **Meet with the domain owner or representative** to demonstrate what they will be presenting to the Army.

Once the chain of command has viewed and approved the datacall, it is time to conduct the datacall, which is Phase III.

PHASE III

CONDUCT THE DATACALL





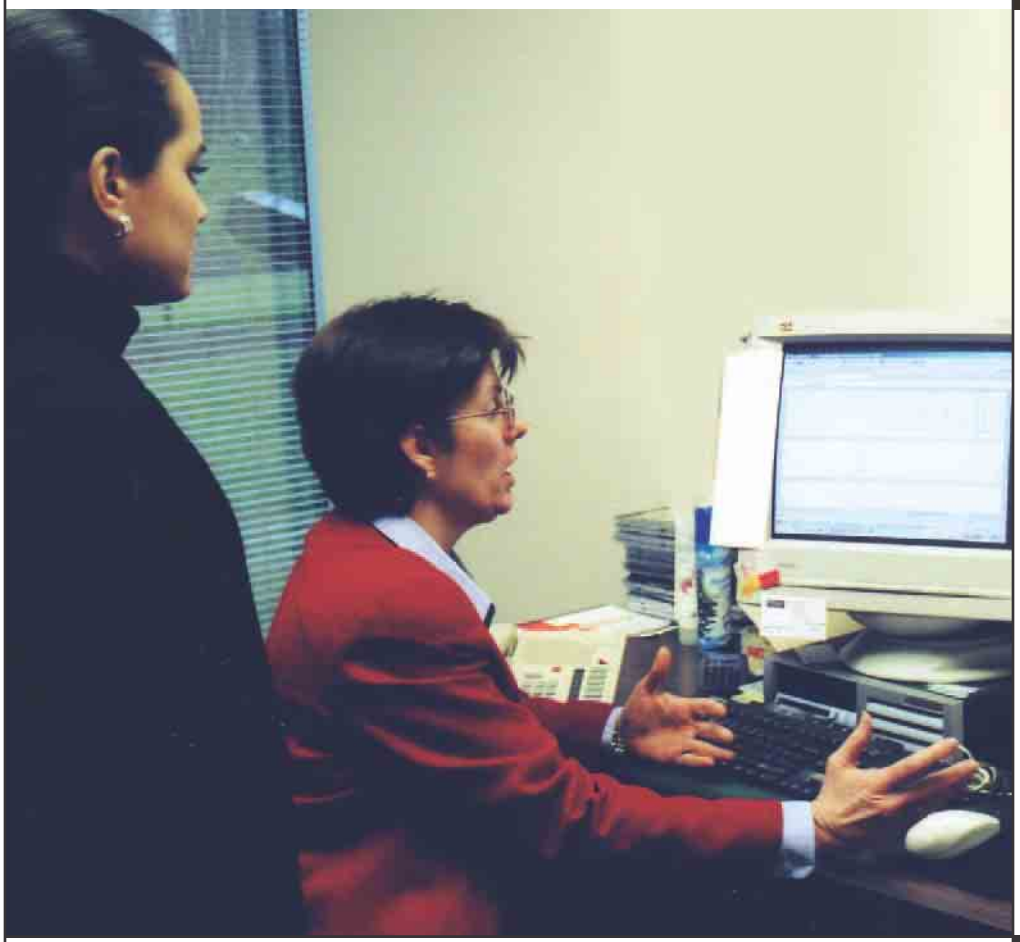
During this phase you will conduct the actual web-based datacall for the length of time determined in Phase II. At the close of Phase III you will be ready to present the datacall results.

The first step in Phase III is to **initiate the datacall.** E-mail the instructions for completing the datacall to each participant. Personalized instructions should include screen names and the website address, as well as the corresponding password.

Regularly **monitor the datacall** to check its completion status. Send out letters (at intervals determined in Phase II) to the commands that have not completed the datacall, reminding them of the number of working days remaining to meet the suspense date. Also, provide your chain of command with a weekly status report. The government point of contact should coordinate frequently with the datacall participants via telephone. These frequent calls to participants can increase the SRAC participation level. Low levels of participation results in a lack of data, which can severely influence both the quality and the results of the datacall.

Staff the datacall help desk throughout the datacall, and ensure attendants can provide any technical and functional support according to fixed customer service standards. If time permits, you can start planning for Phase IV.

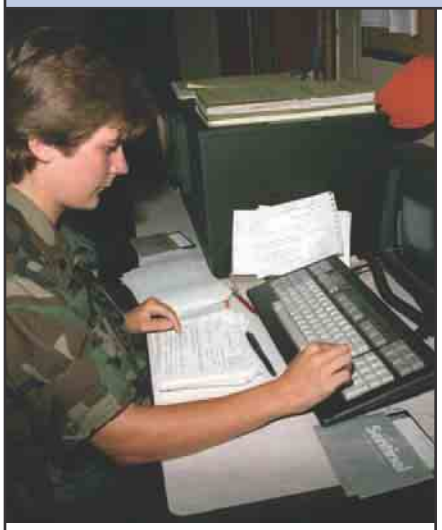
At the conclusion of the datacall, the participation results should be provided to the domain. If the results are not adequate, consider extending the datacall for a short period to capture the required information. Once you **close the datacall** and the domain is satisfied with the participation level, you are ready to categorize and analyze the data in Phase IV.

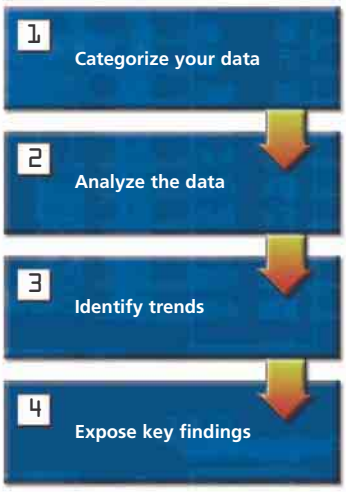


Based on research, established goals, objectives, and any new requirements, the SRAC team should determine the method for presenting the results. An initial review of collected data will determine how to display the final results for the best effect.

PHASE IV

CATEGORIZE AND ANALYZE DATACALL RESULTS





By the end of this phase, you will be ready to produce a final report. In Phase IV you will categorize and analyze the information collected during the datacall.

The first step in this phase is to **categorize your data** according to the types of systems identified in Phase I. For example, if you choose to examine only automated information systems (AIS), you need to examine the updated baseline and categorize the line items according to the type of IT. All other line items (databases, enabling technology, etc.) should be excluded before you analyze the data.

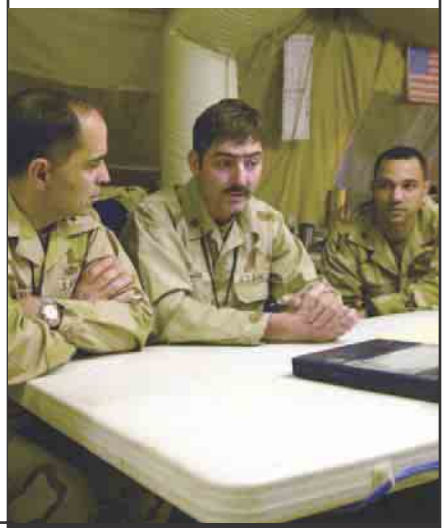
Once all the data entries have been categorized, **analyze the data** based on the type of IT and the system information you need. During analysis, you are looking for trends, issues, and key findings for your final report. The answers to the following questions are typically of interest to a domain:

- Which systems support which functional areas?
- Which systems belong to which domains?
- Which systems are mission-critical or mission-essential?
- Which systems have what kind of technology?
- Which systems have interfaces?
- What kind of technology do the systems with interfaces employ?

- Which systems are unique to the MACOM or organization?
- Which systems are scheduled for consolidation or retirement?

Review the datacall results and **identify trends** that might answer these questions. For example, if more than 50 percent of the systems and databases are used by only one MACOM or organization, it might be important to identify more specific information for MACOM- or organization-unique systems:

- What are the names and descriptions of these unique systems?
- What organization owns the unique systems?
- What functions, sub-functions, and supporting tasks do these unique systems support?
- Are any of these unique systems scheduled for consolidation/ retirement?
  - ✔ Which ones?
  - ✔ When will that occur?
  - ✔ What system, if any, will replace them?

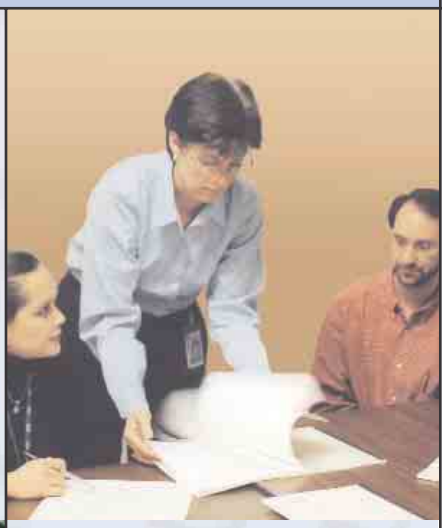


Interfaces might be another area for further analysis. If a high number of interfaces are reported, identify additional information about them based on the data you collected. Consider the following questions:

- How many systems have interfaces that connect to systems that are scheduled for consolidation/retirement?
- How many unique systems have interfaces with systems scheduled for consolidation/retirement?
- How many systems with interfaces are mission-critical?

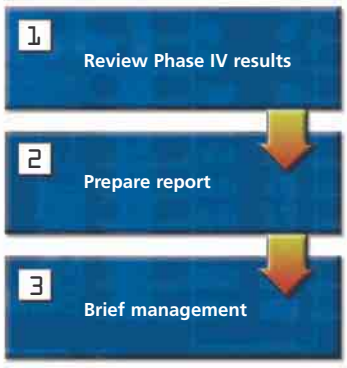
Review of this more defined data will **expose several key findings,** which you can examine further to illustrate your key points. For instance, you can identify supporting tasks and subfunctions to specific systems, show mission essentiality, and indicate systems that should be scheduled for consolidation—all on one chart.

Once the results have been categorized and the analysis is complete, it is time to move to Phase V to consolidate the results and prepare the final report.



PHASE V

CONSOLIDATE RESULTS AND PREPARE FINAL REPORT



During this phase, you will review the information collected in Phase IV and start writing a final report.

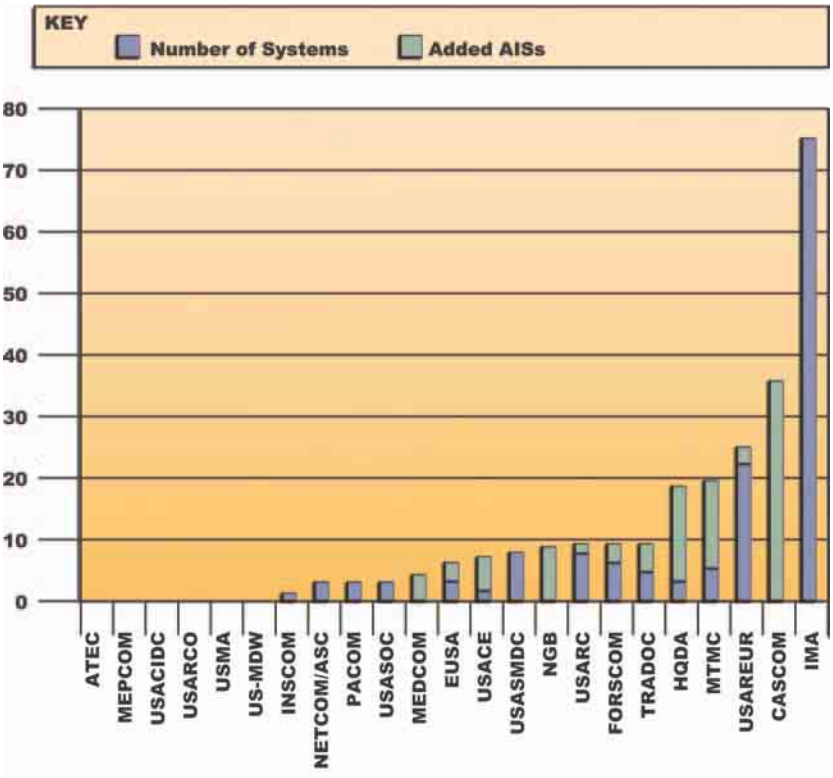
Once you completely **review the results from Phase IV,** you are ready to **prepare your report.** The report can be written in many different formats; however, to get a good picture of the SRAC process, and to document the history of the datacall, consider breaking it into the following three sections, using illustrations wherever applicable:

1. Datacall participation results
2. Datacall results
3. Datacall findings based on the analysis of the data

DATACALL PARTICIPATION RESULTS

When reporting the datacall participation results, present participation statistics—namely how many participants answered the datacall and any significant information that might have contributed to low (or high) participation numbers. Charts can be very effective in displaying complex information across several systems *(See Figure 4)*.

FIGURE 4. SAMPLE DATACALL PARTICIPATION CHART



DATACALL RESULTS

In the next section, present the systems information reported during the datacall. Review how many systems were reported (or added to the datacall) by each participant, and how many systems each participant updated. This section should also convey how many line items you started with, how many you ended with, and how you got from one point to another. *Figure 5* is an example of what information should be conveyed, and how to best convey it.

FIGURE 5. SAMPLE DATACALL RESULTS TABLE

	Adjustment	Balance
+Consolidation		800
-Duplicates	(300)	500
-Non-AIS	(300)	200
+Datacall Results	150	350
-Database	(50)	300
-Enabling Technology	(25)	275
-Other	(150)	125
-Duplicates	(20)	105
-Joint	(10)	95
-DoD	(10)	85
AIS		85

DATACALL FINDINGS

The final portion is the most important part of the datacall. In it, you will summarize key findings, align the findings with the goals and objectives identified in Phase I, and then explain trends that were identified as a result of the analysis in Phase IV, using illustrations where appropriate.

Figure 6 is an example of how data can be displayed in the final report. This chart illustrates the complexity of system functionality. It shows the number of sub-functions or supporting tasks that each system supports and assigns a level of complexity. If you are going to eliminate a system, remember the more functions a system supports, the more interfaces it will have, and the more complex it will be to eliminate. A system supporting only one function may be easier to eliminate or consolidate.

FIGURE 6. SAMPLE ILLUSTRATION OF DATACALL FINDINGS

Other illustrations *(Figure 7 pg. 21)* can graphically answer four of the questions identified in Phase IV.

- Which systems support which sub-functions and supporting tasks?
- Which systems are mission-critical or mission-essential?
- Which systems are unique to the MACOM or organization?
- Which systems are scheduled for consolidation or retirement?

Figures 6 and 7 are just two examples of the many different ways the data can be displayed.

Once the information is collected and the report is written, **prepare a briefing** to the domain owner to describe the findings and the results of the datacall.

FIGURE 7. ALIGNMENT OF SAMPLE WBS AND SYSTEMS ALONG THE MISSION-CRITICAL SPECTRUM

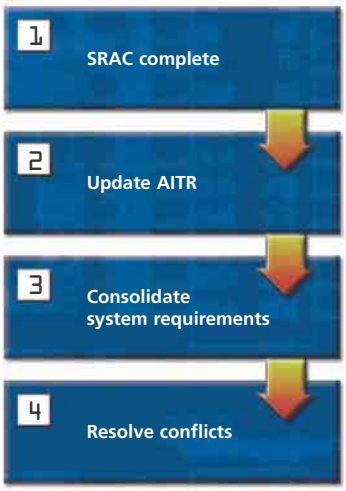
Logistics sub-functions and subordinate tasks	Mission Critical					Mission Essential																									
	URL	GCSS-A	SOAMSS	STMS	WPS	AMS	APPMS	ARSIDS	CAB	FINLO (FORSCOM)	ICARS	IMMC	IRRIS	LIMS	LOGDAT	MOBCON	MSCK-PSMS	MSCK-SMS	MSCK-UMS	PCS	PRISM	REIMS	S2K	SOARrack	TRAPODS	ELAS	ICODES	GOPAX	SABIN	TAMIS	TOPS
1. Manage Requirements	M	X	X	X						X	M				M		M				M	M	M	M	M			X	X		
1.1 Plan requirements	M	X	X	X						M	M						M					M	M	M				X	X		
1.2 Determine requirements	M	X	X	X						M							M				M	M		M				X	X		
1.3 Measure performance	M	X	X	X						X					M		M				M	M	M	M	M						
2. Manage acquisition	M	X		X			M	M		M	M			M			M				M	M	M	M				X	X		
2.1 Acquire items and services	M	X		X				M			M			M			M							M				X	X		
2.2 Acquire technical data and systems										M																					
2.3 Acquire material; and system acquisition							M			M	M			M							M	M	M	M					X		
3. Manage supply/inventory	M	X	X		X		M	M		M	M	M	M	M	M		M				M	M	M	M			X		X	X	
3.1 Manage tactical operations		X						M		M																	X			X	
3.2 Manage national level inventory	M						M			M			M									M									
3.3 Manage national technical data	M				X					M																					
3.4 Manage material storage	M	X	X					M		M	M	M		M	M		M				M	M	M	M			X		X		
4. Manage transportation				X				M			M		M			M											X	X			X
4.1 Authorize transportation				X				M			M					M												X			X
4.2 Manage traffic				X				M					M			M											X				X
4.3 Conduct movement				X												M											X	X			
4.4 Plan maintenance																															
5. Manage maintenance	M	X	X			M						M			M			M	M	M				M		X					
5.1 Perform organization maintenance		X	X			M									M			M	M					M		X					
5.2 Perform intermediate maintenance		X	X			M									M			M	M	M				M		X					
5.3 Perform depot maintenance	M		X									M						M	M	M				M		X					
6. Manage reutilization and marketing							M			M	M	M										M					X		X		
6.1 Maintain item visibility							M			M	M	M										M					X		X		
6.2 Reutilize item										M	M	M																	X		
6.3 Sell item																															
6.4 Scrap and waste item											M																				
7. Manage information resources	M	X					M			M	M				M					M	M	M			M			X	X		X
7.1 Manage information and communication technology																					M							X			
7.2 Develop business applications	M																														
7.3 Manage data	M	X					M			M	M				M					M	M	M			M			X	X		X
8. Manage financial resources	M	X	X				M	M	M	M	M			M	M					M	M	M	M	M	M						
8.1 Plan, program and budget								M	M	M										M			M		M						
8.2 Execute budget and plans	M							M		M																					
8.3 Manage core accounting and general ledger	M							M	M	M																					
8.4 Manage property and assets		X	X				M			M	M			M	M						M	M		M							
9. Manage reporting	M	X	X		X	M	M	M		M	M	M		M	M		M	M	M	M	M	M	M	M	M			X	X		
9.1 Produce internal standard reports	M	X	X		X	M	M	M		M	M	M		M	M		M	M	M	M	M	M	M	M	M				X		
9.2 Produce ad-hoc reports	M	X	X		X	M		M		M	M	M		M	M		M	M	M	M		M	M	M	M			X			
9.3 Produce external reports	M	X	X		X			M		M	M				M		M	M	M	M		M	M	M	M						

Logistics sub-functions and subordinate tasks	Neither										
	ABC	ASER	ELS (19th SC)	IRONSABER	OMA FOI Excess Tracker	Project LIGHTER-ART	PTS	Theater Reparable Tracker	UMSM	ISM-CIF	IMS-CE
1. Manage Requirements	M		M			M	M		M		X
1.1 Plan requirements							M				X
1.2 Determine requirements	M						M				X
1.3 Measure performance	M		M			M	M	M			
2. Manage acquisition							M				
2.1 Acquire items and services							M				
2.2 Acquire technical data and systems							M				
2.3 Acquire material; and system acquisition											
3. Manage supply/inventory	M		M		M	M	M		M	X	X
3.1 Manage tactical operations	M		M			M	M			X	X
3.2 Manage national level inventory											X
3.3 Manage national technical data											
3.4 Manage material storage	M				M				M	X	X
4. Manage transportation											
4.1 Authorize transportation											
4.2 Manage traffic											
4.3 Conduct movement											
4.4 Plan maintenance											
5. Manage maintenance		M	M	M		M			M		
5.1 Perform organization maintenance		M	M	M		M			M		
5.2 Perform intermediate maintenance				M					M		
5.3 Perform depot maintenance											
6. Manage reutilization and marketing	M						M	M			
6.1 Maintain item visibility	M						M	M			
6.2 Reutilize item							M				
6.3 Sell item											
6.4 Scrap and waste item											
7. Manage information resources											
7.1 Manage information and communication technology											
7.2 Develop business applications											
7.3 Manage data											
8. Manage financial resources			M			M	M				
8.1 Plan, program and budget			M			M					
8.2 Execute budget and plans											
8.3 Manage core accounting and general ledger											
8.4 Manage property and assets							M				
9. Manage reporting			M			M	M	M			
9.1 Produce internal standard reports							M				
9.2 Produce ad-hoc reports							M	M			
9.3 Produce external reports			M			M	M				

Logistics sub-functions and subordinate tasks	Scheduled for Consolidation																												
	AMEDDPAS	ARRMS	EDSS	ELS	MEDSS	MMDS	STARTS II	AALPS	ABLCS	AMS (MTMC)	ARSAMS	DAMMS-R BLK III	Enhanced SPBS-R	IBS	LPMAS	SAAS-MOD	SAMS	SARSS-1(O)	SARSS-2AC/2B	SARSS-2AD	SBPS-R	TAMMIS	ULLS-A	ULLS-G	ULLS-S4	VIMS	Total number of systems performing subfunction/supporting task	Number of MACOM-unique systems performing sub-function/supporting task	% of performing systems that are MACOM-uniques
1. Manage Requirements	M	M				M	M	X			X	X	X		X	X	X		X	X		X					35	19	54%
1.1 Plan requirements	M	M				M	M	X			X	X	X			X				X							24	12	
1.2 Determine requirements	M	M				M	M	X			X	X	X						X	X		X					25	12	
1.3 Measure performance	M	M					M				X		X		X		X		X	X		X					27	17	
2. Manage acquisition	M																					X	X				19	13	68%
2.1 Acquire items and services	M																					X	X				14	8	
2.2 Acquire technical data and systems	M																										3	3	
2.3 Acquire material; and system acquisition																						X					10	8	
3. Manage supply/inventory	M	M	M	M		M	M		X		X		X		X	X		X	X	X	X	X	X		X		45	26	58%
3.1 Manage tactical operations			M	M					X		X		X			X		X	X	X	X	X	X		X		23	8	
3.2 Manage national level inventory						M									X			X	X	X	X						12	6	
3.3 Manage national technical data																											3	2	
3.4 Manage material storage	M	M					M				X		X		X	X			X	X		X	X				32	18	
4. Manage transportation		M			M		M	X		X	X	X		X	X	X										M	20	8	40%
4.1 Authorize transportation										X		X				X											9	3	
4.2 Manage traffic										X		X		X	X												11	4	
4.3 Conduct movement					M		M	X		X		X				X											10	2	
4.4 Plan maintenance		M								X	X				X											M	5	2	
5. Manage maintenance	M	M				M					X				X		X					X	X	X			25	16	64%
5.1 Perform organization maintenance	M	M				M					X				X							X	X	X			21	13	
5.2 Perform intermediate maintenance	M	M				M					X				X		X						X	X			19	11	
5.3 Perform depot maintenance	M					M									X								X				12	8	
6. Manage reutilization and marketing	M	M					M			X	X		X									X	X				18	11	61%
6.1 Maintain item visibility		M					M			X	X		X										X				16	10	
6.2 Reutilize item										X			X														7	4	
6.3 Sell item																											0	0	
6.4 Scrap and waste item	M																					X					3	2	
7. Manage information resources		M				M					X		X	X					X	X			X			M	22	12	55%
7.1 Manage information and communication technology														X						X							4	1	
7.2 Develop business applications														X													3	2	
7.3 Manage data		M				M					X		X	X					X	X			X			M	22	12	
8. Manage financial resources	M	M									X		X		X						X	X	X				27	19	70%
8.1 Plan, program and budget	M										X		X		X												12	9	
8.2 Execute budget and plans											X																4	3	
8.3 Manage core accounting and general ledger		M									X												X				7	5	
8.4 Manage property and assets	M	M									X										X	X	X				17	11	
9. Manage reporting	M	M				M	M	X			X	X	X	X	X	X			X	X	X	X	X				43	26	60%
9.1 Produce internal standard reports	M	M				M	M	X			X	X	X	X	X	X			X	X	X	X	X				39	23	
9.2 Produce ad-hoc reports	M	M				M	M				X	X	X	X	X	X			X		X	X	X				36	22	
9.3 Produce external reports	M	M					M	X			X	X	X	X	X	X			X	X	X	X	X				34	19	

Note: M = MACOM-unique system; X = Not MACOM-unique

CONCLUSION



After the **SRAC process is complete,** the next step within the portfolio management process is to **update the AITR.** The CIO/G6 can facilitate the effort to transfer electronic data. The domain manager is responsible for the quality control of the domain's IT systems listed on the AITR, and will coordinate with the other Army domains to resolve any conflicts in system ownership.

Once the data is updated on the AITR, the entire registry should be evaluated. If a system is not on the validated SRAC list, but is on the AITR, it should be scheduled for disposal and removed from the AITR (in collaboration with the system's owner). The CIO/G6 should be able to resolve any issues regarding utilization of systems.

Once the domain's IT systems are added, deleted, or catalogued based on the results of the SRAC process, you are ready to **consolidate systems requirements**—the next step in the portfolio management process. This is the opportunity for the domains to evaluate the legacy IT systems based on the SRAC output. Systems will be evaluated, prioritized, and scheduled for disposal, as appropriate. In this next PfM step you will also review any new initiatives based on new requirements in the strategic plan. Once the decisions are made, an operational architecture can be completed to reflect the domain's decisions.

OSD MEMORANDUM

INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 22 2004

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Information Technology Portfolio Management

Attachment establishes DoD policies and assigns responsibilities for managing information technology (IT) investments as portfolios. Decisions on what IT investments to make, modify or terminate shall be based on architectures, risk tolerance levels, potential returns, outcome goals and performance. While the guidance specifically addresses IT portfolios and a process for making tradeoffs among IT projects, the IT portfolio is part of the Department's broader portfolio of investments. In this larger context, tradeoffs will have to be made between IT and non-IT investments in other agency processes.

This guidance applies to the six Joint Warfighting Capability Assessment areas (i.e., Battlespace Awareness, Command and Control, Force Application, Protection, Focused Logistics, and Net Centricity), the six Business Domains (i.e., Accounting and Finance, Acquisition, Human Resources Management, Installations and Environment, Logistics, and Strategic Planning and Budgeting), and the underlying Enterprise Information Environment. Improved and timely IT investment policies are a cornerstone to enable change throughout the Department, assure that we have the right IT capabilities to perform our mission and conduct effective information operations, eliminate outdated ways of doing business, and achieve our net-centricity goals. While the attached policy is effective immediately, to ensure that this policy is institutionalized, I ask that the DoD Chief Information Officer, in coordination with the Director, Administration and Management, incorporate it into the DoD Directive System within 180 days.

Paul Wolfowitz

Attachment:
As stated

OSD 03246-04

Department of Defense

ASD(NII)/DoD CIO

SUBJECT: Information Technology Portfolio Management

References: (a) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," Revised, (Transmittal Memorandum No. 4), November 28, 2000
(b) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," March 20, 2002
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) Chairman of the Joint Chiefs of Staff Instruction 3170.01, "Joint Capabilities Integration and Development System," June 24, 2003
(e) DoD Directive 5000.1, The Defense Acquisition System," May 12, 2003
(f) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), January 11, 2002

1. PURPOSE

This document:

1.1. Consistent with references (a) and (b) and (c), establishes policies and assigns responsibilities for the management of DoD information technology (IT) and associated investments as portfolios.

1.2. Provides fundamental concepts for managing a portfolio of IT investments that focus on improving business and warfighting outcomes and capabilities.

2. APPLICABILITY AND SCOPE

2.1. This document applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. Joint Warfighting Capability Assessment areas, Business Domains, and the underlying Enterprise Information Environment.

2.1.3. All current and planned IT resources that enable the achievement of Enterprise outcome goals.

3. DEFINITIONS

Terms used in this document are defined in enclosure 1.

4. POLICY

It is DoD policy that:

4.1. Information technology (IT) investments shall be managed as portfolios. Decisions on what IT investments to make, modify or terminate shall be based on the Global Information Grid (GIG) Integrated Architecture, mission area goals, architectures, risk tolerance levels, potential returns, outcome goals and performance.

4.2. Portfolios shall be managed using integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investments strategies.

4.3. Portfolio management processes shall be established and comprised of the following core activities:

4.3.1. Analysis that links Mission Area goals to DoD Enterprise vision, goals, objectives, priorities, capabilities, as well as how these will be achieved and measured; identifies gaps and opportunities; identifies risks and how these will be mitigated; provides for continuous process improvement; and determines strategic direction for mission area activities and processes.

4.3.2. Selection that identifies the best mix of IT investments to achieve outcome goals and plans as well as transition to "to-be" architectures.

4.3.3. Control that ensures a portfolio and individual projects in the portfolio are acquired in accordance with cost, schedule, performance and risk baselines and documented technical criteria, and remain consistent with the current approved version of the GIG Integrated Architecture.

4.3.4. Evaluation that routinely and systematically assesses and measures actual contributions of the portfolio as well as supports adjustments to the mix of portfolio projects, as necessary.

4.4. Integrated Architectures with Enterprise-, Mission Area-, Domain and DoD Component-level perspectives shall be developed, maintained and applied to gain a better understanding of the organization, and the capability gaps between the current and future environments (warfighting and business); assess process improvement opportunities within and across the levels; determine

interoperability and capability requirements; promote standards; identify and implement information assurance requirements; formulate and target investments to improve data and information management; and identify the required capabilities of the technical infrastructure.

4.5. Portfolios shall be nested and integrated at the Enterprise, Mission Area, Domain and DoD Component levels and shall be based on the principles of centralized guidance and oversight, stakeholder participation, collaborative decision making, and decentralized execution.

4.6. Portfolio management processes shall leverage each of the Department's principal decision support systems (i.e., the Joint Capabilities Integration and Development System (reference (d)); Planning, Programming, Budgeting and Execution process; and Defense Acquisition System (reference (e)).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer (DoD CIO), shall:

5.1.1. Establish a process for maximizing the value and assessing and managing the risks of DoD IT investments, consistent with this policy and reference (b).

5.1.2. In coordination with the OSD Principal Staff Assistants, and the Chairman of the Joint Chiefs of Staff, issue procedures for the policies contained herein. This shall include a core set of uniformly applied criteria for portfolio selection and evaluation.

5.1.3. Ensure that integrated architectures (warfighting and business), and their component parts, comply with the GIG Integrated Architecture (reference (c)).

5.1.4. Develop and maintain the DoD Information Resources Management Strategic Plan.

5.1.5. Provide for the enterprise information environment and ensure that its capabilities are synchronized with requirements for these capabilities. This shall include providing for a common set of Enterprise capabilities that enable users (consumers and providers) to discover, access, post, process, advertise, retrieve and fuse data, and make sense of data gathered.

5.1.6. Establish and co-chair, with other senior officials, executive-level governance forums that provide strategic direction, identify opportunities and resolve cross-functional issues that are in the best interest of the Enterprise.

5.2. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall:

5.2.1. Establish policies and procedures to ensure that accounting, financial and asset management, and other related DoD IT business systems are designed, developed, maintained, and

used effectively by the DoD Components to provide financial data reliably, consistently and expeditiously, and support programmatic IT investment decisions, consistent with this policy and reference (b).

5.2.2. In coordination with the DoD CIO and the Principal Staff Assistants, develop and maintain the DoD Business Enterprise Architecture (BEA) and associated Business Enterprise Transition Plan as a component of the GIG Integrated Architecture.

5.2.3. Identify and manage the resolution of cross-cutting issues, facilitate future BEA development, and review budgets and make recommendations to ensure that funds are budgeted to implement the portfolio of BEA projects.

5.2.4. Establish and co-chair, with the DoD CIO, executive-level governance forums that provide strategic direction, identify opportunities and resolve cross-functional issues affecting the business community.

5.3. The Under Secretary of Defense for Acquisition, Technology and Logistics shall ensure policies and procedures contained herein are effectively implemented, consistent with this policy and references (b) and (e).

5.4. The OSD Principal Staff Assistants shall, according to their responsibility and authority for assigned business areas:

5.4.1. Designate Business Domains, in coordination with the DoD CIO and the USD(C)/CFO, and ensure that the following tasks are executed consistent with business enterprise guidance and direction:

5.4.1.1. Establish a repeatable IT portfolio management process, including governance structure(s), consistent with the policies contained herein. This process shall include the core activities described in paragraph 4.3 above, and shall be communicated widely and cascaded down to the DoD Components so that they can understand expectations and effectively participate in the process.

5.4.1.2. Participate in business enterprise governance forums aimed at identifying opportunities for commonality in portfolio management techniques, and providing solutions to problems that are in the best interest of the Enterprise.

5.4.2. In coordination with the DoD CIO, issue policies and procedures that implement the policies contained herein.

5.5. The Director of Program Analysis and Evaluation shall review and issue programming and budgeting guidance that reflects (warfighting and business) portfolio recommendations to continue, modify, terminate or initiate funding for IT projects/programs to ensure compliance with the GIG Integrated Architecture and associated applications.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Perform warfighting mission area control and oversight of supporting information systems, and ensure warfighting mission area leadership throughout the systems' life-cycle phases, consistent with this policy and reference (b).

5.6.2. In coordination with the DoD CIO, issue policies and procedures that implement the policies contained herein, and participate in warfighting enterprise governance forums aimed at identifying opportunities for commonality in portfolio management techniques and providing solutions to problems that are in the best interest of the Enterprise.

5.7. The Heads of the DoD Components shall, as appropriate, execute the tasks described in Paragraphs 5.4 and 5.6 above.

5.8. The DoD Component Chief Information Officers shall provide advice and other assistance to the Component Head and other Component senior management personnel to ensure that information resources are acquired, used, and managed by the DoD Component consistent with the policies contained herein.

6. EFFECTIVE DATE: This document is effective immediately.

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Enterprise Information Environment: The common, integrated computing and communications environment of the Global Information Grid. The GIG EIE is composed of GIG assets that operate as or that assure local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks and wide area networks. The GIG EIE is also composed of GIG assets that operate as or that assure end user devices, work stations and servers that provide local, organizational, regional or global computing capabilities. The GIG EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The GIG EIE includes a common set of Enterprise and mission specific services, called GIG Enterprise Services, which provide awareness of, access to and delivery of information on the GIG.

E1.1.2. Global Information Grid Integrated Architecture. The DoD-wide enterprise architecture that depicts warfighting and business domains.

E1.1.3. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology.

E1.1.4. Information Resources Management. The process of managing information resources to accomplish Agency missions and improve Agency performance, including through the reduction of information collection burdens on the public.

E1.1.5. Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It also includes National Security Systems as defined in reference (b). Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E1.1.6. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, system view, and technical view) that facilitates integration and promotes interoperability across Family-Of-Systems / System-of Systems and compatibility among related mission area architectures (ref (f)).

E1.1.7. Mission Area: A defined area of responsibility whose functions and processes contribute to accomplishment of the mission.

Army Enterprise Integration Oversight Office (AEIOO)

www.army.mil/aeioo